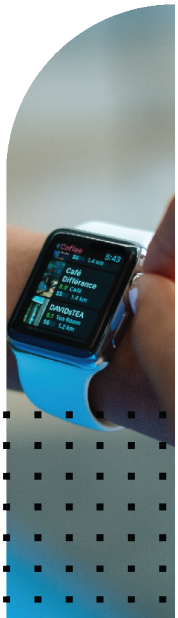
Release Notes

FortiClient (Windows) 7.0.0



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

April 27, 2021
FortiClient (Windows) 7.0.0 Release Notes
04-700-705510-20210427

TABLE OF CONTENTS

Change log

Date	Change Description
2021-04-27	Initial release of 7.0.0.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 7.0.0 build 0029.

Review all sections prior to installing FortiClient.

Licensing

FortiClient 6.2.0+, FortiClient EMS 6.2.0+, and FortiOS 6.2.0+ introduced a new licensing structure for managing endpoints running FortiClient 6.2.0+. See Upgrading from previous FortiClient versions on page 8 for more information on how the licensing changes upon upgrade to 6.2.0+. Fortinet no longer offers a free trial license for three connected FortiClient endpoints on any FortiGate model running FortiOS 6.2.0+. EMS 7.0.0 supports a trial license. With the EMS free trial license, you can provision and manage FortiClient on three Windows, macOS, and Linux endpoints indefinitely. The trial license does not include management of Chromebook endpoints.

FortiClient 7.0.0 offers a free VPN-only version that you can use for VPN-only connectivity to FortiGate devices running FortiOS 5.6 and later versions. You can download the VPN-only application from FortiClient.com. You cannot use the VPN-only client with the FortiClient Single Sign On Mobility Agent (SSOMA). To use VPN and SSOMA together, you must purchase an EMS license.

Special notices

Nested VPN tunnels

FortiClient (Windows) does not support parallel independent VPN connections to different sites. However, FortiClient (Windows) may still establish VPN connection over existing third-party (for example, AT&T Client) VPN connection (nested tunnels).

SSL VPN connectivity issues

Latency or poor network connectivity can affect the FortiClient SSL VPN connection. To further help avoid timeouts, increase the login timeout on the FortiGate to 180 seconds using the following CLI command:

```
config vpn ssl settings
   set login-timeout 180
end
```

Microsoft Windows server support

FortiClient (Windows) supports the AV, vulnerability scan, Web Filter, and SSL VPN features for Microsoft Windows servers.

HP Velocity and Application Firewall

When using an HP computer, a conflict between the HP Velocity application and FortiClient Application Firewall can cause a blue screen of death or network issues. If not using HP Velocity, consider uninstalling it.

Split tunnel

In EMS 6.4.1, application-based split tunneling was configured globally and applied to all IPsec or SSL VPN tunnels. In EMS 6.4.2 and later versions, the application-based split tunneling feature was changed to be configured on a per-tunnel basis. Therefore, a global application-based split tunnel configuration made in EMS 6.4.1 will no longer function after upgrading to 7.0.0. You must complete the per-tunnel configuration after upgrade.

This is unrelated to the FortiOS split tunnel feature.

Installation information

Firmware images and tools

The following files are available in the firmware image file folder:

File	Description
FortiClientTools_7.0.0.xxxx.zip	Zip package containing miscellaneous tools, including VPN automation files.
FortiClientSSOSetup_ 7.0.0.xxxx.zip	FSSO-only installer (32-bit).
FortiClientSSOSetup_ 7.0.0.xxxx_x64.zip	FSSO-only installer (64-bit).
FortiClientVPNSetup_ 7.0.0.xxxx.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_ 7.0.0.xxxx_x64.exe	Free VPN-only installer (64-bit).

EMS 7.0.0 includes the FortiClient (Windows) 7.0.0 standard installer and zip package containing FortiClient.msi and language transforms.

The following tools and files are available in the FortiClientTools_7.0.xx.xxxx.zip file:

File	Description
FortiClientVirusCleaner	Virus cleaner.
OnlineInstaller	Installer files that install the latest FortiClient (Windows) version available.
SSLVPNcmdline	Command line SSL VPN client.
SupportUtils	Includes diagnostic, uninstallation, and reinstallation tools.
VPNAutomation	VPN automation tool.
VC_redist.x64.exe	Microsoft Visual C++ 2015 Redistributable Update (64-bit).
vc_redist.x86.exe	Microsoft Visual C++ 2015 Redistributable Update (86-bit).

The following files are available on FortiClient.com:

File	Description
FortiClientSetup_7.0.0.xxxx.zip	Standard installer package for Windows (32-bit).
FortiClientSetup_7.0.0.xxxx_ x64.zip	Standard installer package for Windows (64-bit).

File	Description
FortiClientVPNSetup_ 7.0.0.xxxx.exe	Free VPN-only installer (32-bit).
FortiClientVPNSetup_ 7.0.0.xxxx_x64.exe	Free VPN-only installer (64-bit).

Review the following sections prior to installing FortiClient version 7.0.0: Introduction on page 5, Special notices on page 6, and Product integration and support on page 9.

Upgrading from previous FortiClient versions

To upgrade a previous FortiClient version to FortiClient 7.0.0, do one of the following:

- Deploy FortiClient 7.0.0 as an upgrade from EMS
- Manually uninstall existing FortiClient version from the device, then install FortiClient (Windows) 7.0.0

FortiClient (Windows) 7.0.0 features are only enabled when connected to EMS 7.0.0.

See the *FortiClient and FortiClient EMS Upgrade Paths* for information on upgrade paths.

Downgrading to previous versions

FortiClient (Windows) 7.0.0 does not support downgrading to previous FortiClient (Windows) versions.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal. After logging in, click *Download* > *Firmware Image Checksums*, enter the image file name, including the extension, and select *Get Checksum Code*.

Product integration and support

The following table lists version 7.0.0 product integration and support information:

Desktop operating systems	• Microsoft Windows 10 (32-bit and 64-bit) • Microsoft Windows 8.1 (32-bit and 64-bit) • Microsoft Windows 7 (32-bit and 64-bit) FortiClient 7.0.0 does not support Microsoft Windows XP and Microsoft Windows Vista.
Server operating systems	• Microsoft Windows Server 2019 • Microsoft Windows Server 2016 • Microsoft Windows Server 2012 R2 • Microsoft Windows Server 2012 • Microsoft Windows Server 2008 R2 FortiClient 7.0.0 does not support Windows Server Core. For Microsoft Windows Server, FortiClient (Windows) supports the Vulnerability Scan, SSL VPN, Web Filter, and AV features, including obtaining a Sandbox signature package for AV scanning. To use SSL VPN on a Windows Server machine, you must enable your browser to accept cookies. Otherwise, tunnel connection fails.
Embedded system operating systems	Microsoft Windows 10 IoT Enterprise LTSC 2019
Minimum system requirements	• Microsoft Windows-compatible computer with Intel processor or equivalent. FortiClient (Windows) does not support ARM-based processors. • Compatible operating system and minimum 512 MB RAM • 600 MB free hard disk space • Native Microsoft TCP/IP communication protocol • Native Microsoft PPP dialer for dialup connections • Ethernet network interface controller (NIC) for network connections • Wireless adapter for wireless network connections • Adobe Acrobat Reader for viewing FortiClient documentation • Windows Installer MSI installer 3.0 or later
AV engine	• 6.00253
FortiAnalyzer	• 7.0.0 and later
FortiAuthenticator	• 6.1.0 and later • 6.0.0 and later
FortiClient EMS	• 7.0.0 and later
FortiManager	• 7.0.0 and later
FortiOS	The following FortiOS version supprts ZTNA with FortiClient (Windows) 7.0.0: • 7.0.0

	The following FortiOS versions support IPsec and SSL VPN with FortiClient (Windows) 7.0.0: • 7.0.0 and later • 6.4.0 and later • 6.2.0 and later • 6.0.0 and later
FortiSandbox	• 3.2.0 and later • 3.1.0 and later • 3.0.0 and later • 2.5.0 and later

Language support

The following table lists FortiClient language support information:

Language	GUI	XML configuration	Documentation
English	Yes	Yes	Yes
Chinese (simplified)	Yes		
Chinese (traditional)	Yes		
French (France)	Yes		
German	Yes		
Japanese	Yes		
Korean	Yes		
Portuguese (Brazil)	Yes		
Russian	Yes		
Spanish (Spain)	Yes		

The FortiClient language setting defaults to the regional language setting configured on the client workstation, unless configured in the XML configuration file.

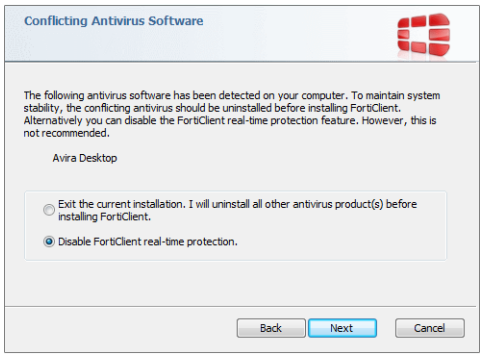
If the client workstation is configured to a regional language setting that FortiClient does not support, it defaults to English.

Conflicts with third party AV products

The AV feature in FortiClient is known to conflict with other similar products in the market.

- You should not use FortiClient's AV feature with other AV products.
- If not using FortiClient's AV feature, you should exclude the FortiClient installation folder from scanning for the third party AV product.

During a new installation of FortiClient, the installer searches for other registered third party software and, if any is found, warns users to uninstall them before proceeding with the installation. There is also an option to disable FortiClient Real Time Protection (RTP).



Resolved issues

The following issues have been fixed in version 7.0.0. For inquiries about a particular bug, contact Customer Service & Support.

Zero Trust Telemetry

Bug ID	Description
687647	Upgrade places FCM in single user mode. Client registrations are blocked due to license limit being reached.
696230	On-fabric detection rule based on public IP address does not recognize IP address change.
697795	FortiClient fails to calculate on-fabric result.
698008	Disconnection from Telemetry also disconnects SSL VPN.
699686	EMS does not receive Software Inventory from FortiClient (Windows).
700357	On-fabric detection does not work after reboot.
704517	FortiClient fails to register to FortiClient Cloud with invitation code.
709445	FortiClient (Windows) reports endpoint is connected when endpoint status is 0.
709723	FortiClient (Windows) ends up without client certificate unless deregistering or reregistering to EMS.
711023	GUI shows incorrect status.

Endpoint control

Bug ID	Description
693087	EMS should show *Owner* for an endpoint device.

Logs

Bug ID	Description
599560	Notification page reports USB block alert source as unknown.

Bug ID	Description
654336	Event log epenfeatures contains firewall, which is disabled.
664452	Endpoint Control logs improvement.
700466	Create proper logs and message when license expires.

Malware Protection and Sandbox

Bug ID	Description
602768	Cloud-based malware detection does not honor allowlisted files.
704823	Antivirus scan does not start.

Remote Access

Bug ID	Description
617420	Remote Access VPN with prelogon without user interaction.
645174	FortiClient sometimes does not use the `remoteauthtimeout` value configured on the FortiGate for SSL VPN.
671392	Windows restart does not remove SSL VPN tunnel that VPN before logon established.
677766	When VPN tunnel goes down, the single host route for the VPN server stays.
682675	SSL VPN users cannot set new PIN after it has expired when using RSA RADIUS authentication.
688043	VPN before logon does not prompt for FortiToken request.
689176	IPsec VPN failover to SSL VPN when using VPN before logon does not work properly.
690769	User cannot start VPN connection with `ENTER` key.
695054	IPsec VPN disconnects right after the tunnel establishes.
695133	DNS resolution is inconsistent when IPv6 is enabled on the desktop.
698177	Public IP address detection and SSL VPN.
706023	FortiClient (Windows) loses DNS settings after restarting computer.

Web Filter and plugin

Bug ID	Description
696581	FortiClient extension pauses download when extension is installed but not in use.

Other

Bug ID	Description
656318	Diagnostics tool uses high CPU, takes a long time to run, and does not finish.
686139	Console fails to open when double-clicking the tray icon.
691564	FortiShield causes third party application performance issues.
691647	Real-time protection GUI event button does not open logs.

Known issues

The following issues have been identified in FortiClient (Windows) 7.0.0. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

FortiSASE SIA

Bug ID	Description
701552	FortiSASE SIA tunnel reconnection issues after FortiSASE SIA portal removes VPN user.

Application Firewall

Bug ID	Description
710910	The *Application Firewall* tab becomes visible after reboot when it should remain hidden.

GUI

Bug ID	Description
708855	GUI shows site is unavailable when blocked.

Endpoint control

Bug ID	Description
699686	EMS does not receive software inventory from FortiClient (Windows).
702660	Switching Active Directory users does not modify user details in EMS *Endpoints* pane.

FSSOMA

Bug ID	Description
705256	SSOMA fails to call WTSQueryUserToken.

Zero Trust Telemetry

Bug ID	Description
587327	Device detection/VPN autoconnect frequency is too often.
652647	FortiClient fails to upload large diagnostics tool result file to EMS.
687611	FortiClient should calculate AD group-based policy rule for tags.
693928	After FortiClient successfully migrates to a new EMS, it does not remove original EMS from EMS list.
697795	FortiClient fails to calculate on-fabric result.
701552	SASE SIA tunnel reconnection issues after SASE SIA portal removes VPN user.
702660	Switching AD users does not modify user details in EMS Endpoints table.
705010	EMS shows endpoints with incorrect usernames.
705664	FortiGate waits about one minute to get `ztna-ems-tag` update.
714131	Migrating FortiClient to a different server fails when connection key is enabled.

Malware Protection and Sandbox

Bug ID	Description
590688	FortiClient says FortiSandbox scan does not support file type when extension is supported and enabled on FortiSandbox.
683027	FortiClient (Windows) shows quarantine message, even if Application Firewall is not installed and quarantine mode will not work.
691328	FortiClient upgrade does not upgrade antivirus engine as deployed through an EMS installer.
705761	FortiClient (Windows) does not block USB drives when removable media access is configured to block WPD devices.
713557	Exceptions do not work for AntiExploit module.

Remote Access

Bug ID	Description
700092	VPN does not connect when using domain user account.
700440	Application-based split tunneling does not work.
702965	Host check interval does not work as expected after PC has previously gone into sleep mode.
703939	FortiClient does not send UID to SSL VPN daemon.
707882	IPsec VPN fails to autoconnect and displays *Failed to launch IPsec service* error.
709001	SSL VPN host check validation does not work for SAML user.
710603	VPN resets with each EMS push.
711227	Per-user autoconnect starts autoconnecting before logging onto Windows.
711402	Per-user autoconnect does not establish and remains connected after logging onto Windows.
713909	If *Enable VPN before Windows* is enabled and there are multiple tunnels configured, there is long delay before Windows login prompt.
714564	SAML connection stays in connecting state and never return with error when FortiGate gateway is inaccessible.

Console

Bug ID	Description
690679	EMS cannot tag endpoints based on nested AD groups.
703213	Reusing/sharing SAML identity provider cookie.
707440	*Clear Logs* button on Settings page is disabled after unlocking settings.

Vulnerability Scan

Bug ID	Description
630202	Vulnerability Scan cannot detect Zoom.exe installer.

Logs

Bug ID	Description
709729	realtime_scan log disappears after ten seconds.

Other

Bug ID	Description
69182	FortiClient does not support the pound (£) sign.
689936	GUI issue when connecting to IPsec VPN using FortiTray.

www.fortinet.com